UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

TREVOR SLOAN, JOSEPH BLEIBERG, ARYEH LOUIS ROTHBERGER, PATRICK COMMERFORD, KEVIN FARR, ELMER ORPILLA, KEITH LAPATIN, and SAGAR DESAI, on behalf of themselves and all others similarly situated,	)	
Plaintiffs,	)	No. 22 C 7174
v.	)	Judge Sara L. Ellis
ANKER INNOVATIONS LIMITED, FANTASIA TRADING LLC, and POWER MOBILE LIFE LLC,	)	
Defendants,	)	

OPINION AND ORDER

Plaintiffs Trevor Sloan, Joseph Bleiberg, Aryeh Louis Rothberger, Patrick Commerford, Kevin Farr, Elmer Orpilla, Keith Lapating, and Sagar Desai allege Defendants Anker Innovations Limited ("Anker"), Fantasia Trading LLC ("Fantasia"), and Power Mobile Life LLC ("Power Mobile") violated various privacy laws relating to their practices in storing data connected to their "eufy" branded security products.[1] Among other claims, Plaintiffs allege that Defendants violated the Illinois Biometric Information Privacy Act ("BIPA"), 740 Ill. Comp. Stat. 14/1 *et seq*.

On January 9, 2024, this Court granted in part and denied in part Defendants' motion to dismiss Plaintiffs' consolidated complaint. Doc. 66. Among other rulings, the Court dismissed all non-Illinois resident Plaintiffs from the BIPA claim, and only permitted Sloan, Orpilla, and the Illinois-resident class members' (together, the "BIPA Plaintiffs") BIPA claim to proceed.

[1] On May 8, 2023, the Court consolidated this case with *Bleiberg v. Anker Innovations Ltd.*, No. 22 C 7218 (N.D. Ill.), and *Desai v. Anker Technology Corp.*, No. 23 C 1607 (N.D. Ill), for all purposes.

Now, Defendants move to dismiss the BIPA Plaintiffs' BIPA claim under Federal Rule of Civil Procedure 12(c). Because the BIPA Plaintiffs allege that the transaction giving rise to their BIPA claim occurred primarily and substantially in Illinois, the Court denies Defendants' motion [99].

BACKGROUND

Plaintiffs' claims arise from their purchase and use of Defendants' "eufy" branded security products, specifically eufy home security cameras and video doorbells (the "eufy products"). Doc 31 at 1. The eufy products can access Wi-Fi, record and stream video, and detect motion. The eufy products apply a facial recognition program called the BionicMind system, which differentiates between known individuals and strangers by recognizing biometric identifiers and comparing the face template against those stored in a database. The eufy products sync to a consumer's phone through the eufy Security app.

Anker's marketing for the eufy products stated that "the products saved all video recordings and conducted all facial recognition locally (meaning on equipment located with and controlled by the consumer)." *Id.* at 2 (emphasis omitted). Specifically, the eufy products' labels advertise that information is "[s]tored locally[] [w]ith military-grade encryption" and "transmitted to you, and only you." *Id.* at 17. Anker's website includes additional statements like: "Our AI is built in to your security devices. It analyzes recorded video locally without the need to send it to the cloud for analysis." *Id.* And, "[w]ith secure local storage, your private data never leaves the safety of your home, and is accessible by you alone." *Id.* at 18. Further, Anker's privacy policy, also available on its website, does not disclose to customers that "Defendants will collect, transmit, and disseminate [customer's] images and biometric information (i.e., face templates) to third parties." *Id.* at 19.

The BIPA Plaintiffs all purchased at least one eufy product between June 2020 and November 2022 and installed them in their respective residences in Illinois. Further, the BIPA Plaintiffs allege that they did not consent to Defendants transmitting, uploading, or storing their biometric information, nor did they receive a retention schedule or policy concerning their biometric data.

In November 2022, Paul Moore, a security researcher, posted several tweets and videos revealing holes in the security network for the eufy products. Specifically, Moore identified that the eufy products uploaded "images and facial recognition data to Defendants' cloud storage, which is hosted by a third party (Amazon Web Services ('AWS'), a subsidiary of Amazon.com, Inc.)." *Id.* at 3. Moore determined that he could stream content from his videos through unencrypted websites and posted a video showing that he could access his camera feed through an incognito web browser. SEC Consult, a security firm, and *The Verge*, an online technology media outlet, confirmed Moore's results. When Moore emailed eufy, a eufy employee wrote in an email that "the app needs to communicate with the cloud server in real-time" in a manner "referring to the transmittal of images to Defendants' cloud storage and application of facial recognition technology to such images on the cloud." *Id.* at 26 (emphasis omitted).

Defendants initially denied that the eufy products streamed video without encryption. However, on November 29, 2022, Defendants released a statement asserting that "[a]lthough our eufy Security app allows users to choose between text-based or thumbnail-based push notifications, it was not made clear that choosing thumbnail-based notifications would require preview images to be briefly hosted on the cloud. The lack of communication was an oversight on our part and we sincerely apologize for the error." *Id.* at 26. Several months later, in January 2023, Anker's global head of communication provided a statement to *The Verge* acknowledging

prior denials from the company regarding the production of unencrypted videos were wrong and that the unencrypted video streams were "a known issue, easily replicated and had been reported by the media." *Id.* at 28.

LEGAL STANDARD

"A motion for judgment on the pleadings under Rule 12(c) of the Federal Rules of Civil Procedure is governed by the same standards as a motion to dismiss for failure to state a claim under Rule 12(b)(6)." *Adams v. City of Indianapolis*, 742 F.3d 720, 727–28 (7th Cir. 2014); *see also Federated Mut. Ins. Co. v. Coyle*, 983 F.3d 307, 313 (7th Cir. 2020) ("The only difference between a motion for judgment on pleadings and a motion to dismiss is timing; the standard is the same."). A motion to dismiss under Rule 12(b)(6) challenges the sufficiency of the complaint, not its merits. Fed. R. Civ. P. 12(b)(6); *Gibson v. City of Chicago*, 910 F.2d 1510, 1520 (7th Cir. 1990). In considering a Rule 12(b)(6) motion to dismiss, the Court accepts as true all well-pleaded facts in the plaintiff's complaint and draws all reasonable inferences from those facts in the plaintiff's favor. *AnchorBank, FSB v. Hofer*, 649 F.3d 610, 614 (7th Cir. 2011). To survive a Rule 12(b)(6) motion, the complaint must not only provide the defendant with fair notice of a claim's basis but must also be facially plausible. *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009); *see also Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555, 127 S. Ct. 1955, 167 L. Ed. 2d 929 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678.

ANALYSIS

Defendants argue that the BIPA Plaintiffs' claim must fail because they have not adequately alleged that the unauthorized collection and transmission of their biometric

information occurred primarily and substantially in Illinois. More specifically, Defendants argue that the BIPA Plaintiffs have not pleaded a legally actionable BIPA claim under extraterritoriality principles because the BIPA Plaintiffs do not allege that the eufy products themselves collect or process biometric information at their residences in Illinois, but rather that the eufy products send "unprocessed photographs" to servers outside of Illinois where the images are then used to remotely generate the BIPA Plaintiffs' facial geometry.

I. Judicial Notice

First, Defendants ask the Court to take judicial notice of AWS's website, which supposedly states that AWS does not possess any cloud infrastructure or servers in Illinois. Defendants direct the Court to AWS's "Regions and Availability Zones" webpage (the "AWS website"). *See Regions and Availability Zones*, AWS, https://aws.amazon.com/about-aws/global-infrastructure/regions_az/ (last accessed July 24, 2025).

The Court finds that taking judicial notice of the AWS website is not appropriate at this time and, even if it was, that the webpage does not support Defendants' asserted claim that AWS does not possess any servers in Illinois. A court may take judicial notice of a fact that "is not subject to reasonable dispute because it (1) is generally known within the trial court's territorial jurisdiction; or (2) can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201. Courts may take judicial notice of the content of websites. *See, e.g.*, *Gilsinger v. Cities & Villages Mut. Ins. Co.*, 693 F. Supp. 3d 975, (E.D. Wis. 2023) ("[T]he Court may take judicial notice of public record information obtained from an official government website."). However, judicial notice is not appropriate in this instance because the parties dispute whether AWS maintains infrastructure in Illinois and AWS does not

make any authoritative representations on the AWS website that it is conclusively listing the locations of all of its cloud infrastructure or servers.

Further, the Court notes that under both the currently accessible version of the AWS website and the screenshots of the AWS website that Defendants provided of how it appeared at the time they filed their brief, the AWS website indicates that AWS does have some infrastructure in Illinois, and it is unclear if that infrastructure is cloud infrastructure or servers. On Defendants' screenshot of the AWS website, AWS includes "Chicago, IL" on its list of "Edge locations" and "Chicago" on its list of AWS Local Zones. Doc. 104-1 at 12. The AWS webpage does not define edge locations, but it defines "Local Zones" as locations that "place compute[r], storage, database, and other select AWS services." *Id.* Under the current version of the AWS website, the "Edge Locations" heading states that "[t]he AWS Cloud in North America has 31 Availability Zones within 9 Geographic Regions, with 31 Edge Network Locations and 3 Edge Cache Locations." *Regions and Availability Zones*, AWS, https://aws.amazon.com/about-aws/global-infrastructure/regions_az/ (last accessed July 24, 2025). Following that information, the AWS website lists 31 cities, including "Chicago, IL." Further, the AWS website describes "Availability Zones" as "one or more discrete data centers with redundant power, networking and connectivity in an AWS Region." *Id.* Altogether, the AWS website repeatedly references Chicago, Illinois as a location that contains some services, and potentially infrastructure, for AWS. This information undermines Defendants' assertion that AWS does not possess any cloud infrastructure or servers in Illinois, and supports that a dispute exists on this issue. Because a reasonable dispute exists about the meaning of the AWS website and whether AWS possesses infrastructure in Illinois, the Court does not find it appropriate to take judicial notice of the AWS website. *See Van Tassell v. United Mktg. Grp., LLC*, 795 F. Supp. 2d 770, 780 (N.D. Ill. 2011)

(finding that it was not appropriate to take judicial notice of a webpage where the plaintiffs disputed the authenticity and accuracy of the webpage such that the webpage did not indisputably support the proposition that defendants asserted it supported).

II. Sufficiency of the Allegations

Next, the Court turns to whether the BIPA Plaintiffs have a plausible claim against Defendants, or whether extraterritoriality principles bar their claims. BIPA makes it unlawful to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers and/or biometric information" without a written release. 740 Ill. Comp. Stat. 14/15(b). BIPA further requires that "[a] private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied." 740 Ill. Comp. Stat. 14/15(a). BIPA defines biometric identifiers as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 Ill. Comp. Stat. 14/10. The biometric identifier definition excludes photographs. *Id.* BIPA defines biometric information as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.* The biometric information definition excludes "information derived from items or procedures excluded under the definition of biometric identifiers." *Id.*

Under Illinois law, "a statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute." *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 184–85 (2005) (citation omitted). Because "none of BIPA's express provisions indicates that the statute was intended to have extraterritorial effect . . . BIPA does not

apply extraterritorially." *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017). To avoid the extraterritoriality doctrine, "the circumstances that relate to the disputed transaction [must have] occur[red] primarily and substantially in Illinois," with "each case . . . decided on its own facts." *Avery*, 216 Ill. 2d at 187.

Further, while photographs alone do not support a BIPA action, photographs used by a system that can take a geometric scan of a person do qualify as biometric data. *Sosa v. Onfido, Inc.*, 600 F. Supp. 3d 859, 871 (N.D. Ill. 2022) (determining that faceprints—scans of identification cards and photographs—qualify as biometric identifiers because they "plausibly constitute scans of face geometry"). This is because "a 'biometric identifier' is not the underlying medium itself, or a way of taking measurements, but instead is a set of measurements of a specified physical component (eye, finger, voice, hand, face) used to identify a person." *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017); *see also Sosa*, 600 F. Supp. 3d at 871 ("But nothing in section 10 expressly excludes information derived from photographs from the definition of biometric identifiers.").

Here, Defendants argue that the BIPA Plaintiffs' claims run afoul of extraterritoriality requirements because "Plaintiffs allege their cameras collected a photograph—not biometric data—and then transferred that photograph to the AWS cloud where it was subjected to facial recognition technology that generated biometric data for the first time." Doc. 104 at 9. In other words, Defendants argue that the alleged BIPA violations did not occur primarily and substantially in Illinois because the BIPA Plaintiffs' photos did not become biometric identifiers until they were outside of Illinois in the AWS cloud servers.

Defendants' argument misconstrues the allegations in the consolidated complaint. The BIPA Plaintiffs do not allege that the eufy products only collected their photos, sent those photos

to AWS, and then AWS processed those photos into biometric information for the first time outside of Illinois. Rather, the BIPA Plaintiffs allege that the BionicMind system in the eufy products "allows eufy cameras to differentiate between known individuals and strangers by recognizing biometric identifiers" and that the eufy products "upload images and facial recognition data to Defendants' cloud storage." Doc. 31 at 3, 15. The BIPA Plaintiffs reiterate this same claim multiple times throughout the amended complaint. *See, e.g.*, *id.* at 1 ("The [eufy] Products are equipped with . . . facial recognition[.]"); *id.* at 3 ("Anker was not only storing facial recognition data in the cloud, but also sharing that back-end information between accounts."); *id.* at 6 ("Had Sloan known the Camera Products captured biometric data and uploaded pictures and video online to Anker's servers . . . ."); *id.* at 26 ("Defendants eventually admitted that they were already aware that their eufy cameras transmitted images and biometric information to their AWS-hosted cloud storage.").

The Court notes that the consolidated complaint does contain some allegations that suggest that the eufy products also sent photographs, which are not themselves biometric identifiers, to AWS, which then used software to convert those photos into biometric information. *See, e.g.*, *id.* at 26 ("[R]eferring to the transmittal of images to Defendants' cloud storage and the application of facial recognition technology to such images on the cloud."). However, the BIPA Plaintiffs make these allegations in addition to their other allegations about the eufy products performing facial recognition themselves and transferring facial recognition data. The Court is satisfied that the BIPA Plaintiffs have adequately alleged that the circumstances making up each transaction occurred primarily and substantially in Illinois because they allege that the access to their biometric identifiers without their consent occurred at their residences, where they installed the cameras. *See Smith v. Signature Sys., Inc.*, No. 21 C

20205, 2022 WL 595707, at *3 (N.D. Ill. Feb. 28, 2022) (extraterritoriality doctrine did not bar claim where complaint alleged that BIPA violations occurred in Illinois); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1276 (9th Cir. 2019) ("[I]t is reasonable to infer that the General Assembly contemplated BIPA's application to individuals who are located in Illinois, even if some relevant activities occur outside the state."); *cf. Neals v. PAR Tech. Co.*, 419 F. Supp. 3d 1088, 1091 (N.D. Ill. 2019) ("[I]n light of the fact that Neals does not specify the location of the Charley's Philly Steaks at which she worked, the Court is unable to reasonably infer from the complaint that her fingerprint was collected in Illinois. If plaintiff were able to so allege, then she would sufficiently allege facts indicating that the circumstances relating to the alleged transaction occurred primarily and substantially in Illinois; the transaction would allegedly involve an Illinois resident having her biometric information collected in Illinois by a private entity, without the entity's having provided the requisite disclosures and obtained the requisite consent there.").

The three cases Defendants rely on to support their claim that the BIPA Plaintiffs did not allege adequate BIPA claims are also inapposite because Defendants again ignore that the BIPA Plaintiffs allege that Defendants collected their biometric information through their eufy products in Illinois. Thus, the cases Defendants cite did not involve any "allegation that the plaintiffs' biometric information was 'actually collected in Illinois'" *Campana v. Nuance, Commc'ns, Inc.*, No. 21 C 1241, 2024 WL 2809838, at *2 (N.D. Ill. Mar. 8, 2024); *see also McGoveran v. Amazon Web Servs., Inc.*, No. 1:20-cv-01399, 2024 WL 4626253, at *5 (D. Del. Oct. 30, 2024) (finding that the alleged transaction had not occurred in Illinois because the defendant did not create or collect the biometric information in Illinois, rather the plaintiffs made phone calls from Illinois and the biometric information was created elsewhere); *Vance v. Google LLC*, No. 20-cv-4696, 2024 WL 1141007, at *3 (N.D. Cal. Mar. 15, 2024) (finding that the

alleged transaction had not occurred primarily and substantially in Illinois where plaintiffs in Illinois uploaded their photos to a website and then a New York company turned those photos into facial geometry). Here, because the BIPA Plaintiffs allege that the eufy products collected their biometric information in Illinois, the Court finds that extraterritoriality principles do not bar the BIPA Plaintiffs' BIPA claim.

CONCLUSION

Because the BIPA Plaintiffs state a claim, the Court denies Defendants' motion for judgment on the pleadings [99].

Dated: July 28, 2025

SARA L. ELLIS
United States District Judge